UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

AMERICAN FURUKAWA, INC.,

Plaintiff,

v.

ISTHIHAR HOSSAIN,

Defendant.
_____/

Case No. 14-cv-13633

UNITED STATES DISTRICT COURT JUDGE
GERSHWIN A. DRAIN

UNITED STATES MAGISTRATE JUDGE
MICHAEL J. HLUCHANIUK

OPINION AND ORDER DENYING DEFENDANT'S MOTION FOR PARTIAL JUDGMENT ON THE PLEADINGS [30]

I. INTRODUCTION

American Furukawa, Inc. ("Furukawa" or "Plaintiff") commenced the instant action against its former employee, Isthihar Hossain ("Defendant"), on September 19, 2014. *See* Dkt. No. 1. In the Complaint, Furukawa alleges that Hossain unlawfully accessed its computers to obtain confidential information in violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030. Additionally, Furukawa brings claims under Michigan law for Fraud, Breach of Contract, Breach of Fiduciary Duty, Misappropriation of Trade Secrets, and Conversion. *Id.*

When it filed the Complaint, Furukawa simultaneously moved for a Temporary Restraining Order ("TRO"). *See* Dkt. No. 4. On September 22, 2014, the Court entered a TRO enjoining Hossain from using Furukawa's information, and ordering Hossain to show cause why a preliminary injunction should not be issued; account for and return Furukawa's confidential information; and abide by a confidentiality agreement between the parties. *See* Dkt. No. 7. The parties entered a Stipulated Order leaving the terms of the TRO in place, while setting forth an agreed protocol for examining the computers and email accounts at issue. *See* Dkt. No. 18.

Presently before the Court is Defendant's Partial Motion for Judgment on the Pleadings Pursuant to Rule 12(c) of the Federal Rules of Civil Procedure. *See* Dkt. No. 30. Furukawa filed a Response to Hossain's Motion, but Hossain failed to file a Reply in accordance with the Court's Local Rules. *See* E.D. Mich. L.R. 7.1(e)(1)(c). After reviewing the briefing, the Court concludes that oral argument will not aid in the resolution of this matter. Accordingly, the Court will resolve the Motion on the briefs as submitted. *See* E.D. Mich. L.R. 7.1(f)(2). For the reasons discussed herein, the Court will **DENY** Hossain's Motion for Partial Judgment on the Pleadings Pursuant to Rule 12(c) of the Federal Rules of Civil Procedure [30].

II. FACTUAL BACKGROUND

American Furukawa, Inc. is a Delaware corporation and its principal place of business is located at 47677 Galleon Ct, Plymouth, Michigan. Furukawa is a supplier of advanced technology automotive, electronics and specialty products to several high technology industries. Isthihar Hossain accepted employment with Furukawa in September, 2011 as a Power Systems Electrical Engineer. Hossain reported to Furukawa's General Manager and Vice President.

When Hossain began his employment with Furukawa, Furukawa asserts that Hossain agreed to abide by Furukawa's Policies regarding "Supplier and Vendor Information," "Conflicts of Interest," "Confidentiality," "Outside Employment," "Company Property" and "Removable Media Use." Furukawa also asserts that Hossain entered into an Invention Assignment & Secrecy Agreement ("Secrecy Agreement") with Furukawa, which dictated that Hossain "will regard and preserve as confidential all trade secrets pertaining to the Company's business that have been or may be obtained by me by reason of my employment." The Secrecy Agreement also dictated that Hossain would not "without prior authority from the Company to do so, use for

my own benefit or purposes, nor disclose to others, either during my employment or thereafter" any trade secrets pertaining to Furukawa's business.

By 2014, Hossain had become a Production Manager and Senior Production Manager with access to Furukawa's trade secrets, know-how, intellectual property and other confidential information. On March 11, 2014, while he was still employed by Furukawa, Furukawa asserts that Hossain entered into an "Employment Agreement" ("Agreement") with Huatong—a competitor and supplier to Furukawa. As part of Hossain's alleged Agreement with Huatong, Hossain was to serve as CEO of a new sales company, American Huatong. Also on March 11, Furukawa asserts that Hossain downloaded 910 Furukawa files to his external hard drive without his manager's permission.

On March 14, 2014, Furukawa states that Hossain called into Furukawa's offices and indicated he was sick. Yet, on March 17, 2014, Furukawa asserts that Hossain downloaded another 875 Furukawa files and also moved two-and-a-half years of email from Furukawa's exchange server to his external hard drive without his manager's permission. While files were allegedly being downloaded on March 17, 2014, Furukawa states that Hossain informed Furukawa he was unable to work due to a basketball injury. Notably, pursuant to his alleged Agreement with Huatong, Hossain was scheduled to begin his employment with Huatong on March 17, 2014.

As a result of his reported injury, Hossain was granted a leave of absence, commencing March 18, 2014. Critically, as a condition for granting the leave of absence, Furukawa asserts that it instructed Hossain that he could not do "any work" for Furukawa during his leave of absence. Despite the instructions to the contrary, Furukawa asserts that Hossain accessed information on his company laptop and copied Furukawa files from his company email to his

personal "gmail" account during his leave of absence. Furukawa purportedly did not learn of Hossain's activities until the following chain of events raised suspicion.

On March 20, 2014, Huatong announced that it would no longer sell Electrical Submersible Pump ("ESP") cables to the United States market through a partnership with Furukawa. Huatong also announced that it would no longer sell service drop cables to Kingwire, and photovoltaic ("PV") cables to the United States market, through Furukawa.

On Thursday, April 24, 2014, Hossain sent an email to Furukawa's Manager of Human Resources stating that his doctor had cleared him to return to work. On April 25, 2014, Furukawa claims Hossain reported for work late and left early. On Monday, April 28, 2014, Hossain announced that he was resigning his employment, effective May 2, 2014. Furukawa accepted Hossain's resignation, effective April 29, 2014, and paid him through May 2, 2014.

Despite his alleged Agreement with Huatong, when he resigned his employment, Hossain allegedly indicated he did not "have another job lined up or anything," but his "previous employer" had been contacting him, and he was "pretty sure" that he could get a job with them. Upon his departure from Furukawa, Hossain was asked to sign an "Employee Certification & Agreement on Termination," certifying that he had returned all property belonging to the Company, had complied with the Secrecy Agreement and would continue to abide by that Agreement. Hossain allegedly refused to sign.

On or about May 12, 2014, Furukawa learned that Huatong had approached WTEC—one of Furukawa's customers—about buying cable from Huatong. On May 16, 2014, Furukawa received an email from WTEC regarding WTEC's "compound" requirements and "payment terms." The email from WTEC was addressed to Hossain at his former Furukawa email address. On May 30, 2014, WTEC confirmed that Hossain was acting as Huatong's agent with respect to

the sales negotiations between WTEC and Huatong. On June 5, 2014, Furukawa received another email from WTEC, addressed to Hossain's Furukawa email address purportedly asking Hossain to quote the price for "PV Wire 2kV AL S-8000" and "PV Wire 2kV CU."

Furukawa sent a letter to Hossain on June 9, 2014, reminding him of his obligations under the Secrecy Agreement. In the letter, Furukawa demanded that Hossain immediately cease and desist from any further solicitation of cable business from WTEC or any other customer of Furukawa. Furukawa also sought assurances that Hossain would abide by his trade secret obligations, and would not use or disclose any trade secret information that he acquired during his employment with Furukawa. Hossain purportedly refused to comply with this request. Furukawa attempted to negotiate with Hossain to resolve the dispute. Throughout the negotiations, Hossain purportedly maintained that he had returned all property belonging to Furukawa and fully complied with the Secrecy Agreement. After looking into the actions of Hossain, Furukawa brought the instant action pursuant to the CFAA and Michigan law.

III. DISCUSSION

A. LEGAL STANDARD

Federal courts review motions for judgment on the pleadings brought pursuant to Federal Rule of Civil Procedure 12(c) using the standards applicable to motions filed under Rule 12(b)(6). *See Wee Care Child Ctr., Inc. v. Lumpkin*, 680 F.3d 841, 846 (6th Cir. 2012). Though litigants employ these procedural mechanisms at different stages of the proceedings, the purpose of both motions is to test the legal sufficiency of a plaintiff's pleadings. Thus, as with Rule 12(b)(6) motions, a Rule 12(c) motion allows a court to make an assessment as to whether a plaintiff has stated a claim upon which relief can be granted. Fed. R. Civ. P. 12(b)(6).

As articulated by the Supreme Court of the United States, "[t]o survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to

relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 554, 570, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007)). This facial plausibility standard requires claimants to put forth "enough fact[s] to raise a reasonable expectation that discovery will reveal evidence of" the requisite elements of their claims. *Twombly*, 550 U.S. at 557. Even though a complaint need not contain "detailed" factual allegations, its "factual allegations must be enough to raise a right to relief above the speculative level." *Ass'n of Cleveland Fire Fighters v. City of Cleveland*, 502 F.3d 545, 548 (6th Cir. 2007) (citing *Twombly*, 550 U.S. at 555) (internal citations omitted).

While courts are required to accept the factual allegations in a complaint as true, *Twombly*, 550 U.S. at 556, the presumption of truth does not apply to a claimant's legal conclusions, *Iqbal*, 556 U.S. at 678. Therefore, to survive a motion to dismiss, a plaintiff's pleading for relief must provide "more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Ass'n of Cleveland Fire Fighters*, 502 F.3d at 548 (quoting *Twombly*, 550 U.S. at 555) (internal citations and quotations omitted).

In addition to evaluating the sufficiency of the factual allegations within the four corners of a complaint, courts may consider any exhibits attached to the complaint, matters of public record, and exhibits attached to a defendant's 12(b)(6) motion, provided that the latter are referred to in the complaint and are central to the claims therein. *See Bassett v. NCAA*, 528 F.3d 426, 430 (6th Cir. 2008) (citing *Amini v. Oberlin Coll.*, 259 F.3d 493, 502 (6th Cir. 2001)).

B. LEGAL ANALYSIS

The central question presented by Hossain's Motion is whether this Court should adopt the approach taken by other district courts in Michigan to find that Hossain did not violate the CFAA when he removed files from Furukawa servers in contravention of a confidentiality agreement and computer policy.

The Court must also resolve the following questions presented by Hossain' Motion: whether the Michigan Uniform Trade Secrets Act ("MUTSA") preempts Furukawa's claims for Fraud, Breach of Contract, Breach of Fiduciary Duty, and Conversion; whether Furukawa's Breach of Contract claim is precluded by disclaimer language in the Furukawa Policies and Practices Handbook; and whether Furukawa can bring a claim for Conversion.

With respect to the central question advanced in Hossain's Motion, the Court navigated a deep circuit split regarding interpretations of the CFAA's phrases "without authorization" and "exceeds authorized access." The Sixth Circuit has given separate meaning to both of these phrases. Following the Sixth Circuit's guidance, this Court finds that Furukawa has stated a proper claim under the CFAA, because Furukawa has plead that Hossain accessed some files when he was told not to work for Furukawa—"without authorization"—and accessed other files in in violation of a computer policy—"exceeds authorized access."

With respect to the remaining questions presented by Hossain's Motion, the Court finds that Furukawa's claims under Michigan law are not preempted by MUTSA because Furukawa's claims are not based *solely* on trade secrets. Additionally, the Court finds that Furukawa's Breach of Contract claim is not premised on the Furukawa Policies and Practices Handbook, so the handbook does not warrant the dismissal of Furukawa's claim. Lastly, the Court finds that Furukawa has presented a proper claim for Conversion because Hossain took information from Furukawa's servers. The Court's findings are addressed in detail below.

1. Furukawa Properly Asserts Claims Under the CFAA

The CFAA prohibits seven types of conduct involving unauthorized access to computers. *See* 18 U.S.C. § 1030(a)(1)-(7). While the CFAA was initially just a criminal statute, in 1994 Congress added private civil causes of action to permit "[a]ny person who suffers damage or loss by reason of a violation of [the statute]" to "maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).

Furukawa contends that Hossain violated 18 U.S.C. § 1030(a)(2)(c) ("Subsection (a)(2)(c) of the CFAA"), which imputes liability to anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." 18 U.S.C. § 1030(a)(2)(c). Additionally, Furukawa asserts that Hossain violated 18 U.S.C. § 1030(a)(4) ("Subsection (a)(4) of the CFAA"), which imputes liability to anyone who "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value[.]" 18 U.S.C. § 1030(a)(4).

Under both Subsection (a)(2)(c) and Subsection (a)(4) of the CFAA, Hossain would be liable if Furukawa is able to demonstrate that he accessed a "protected computer"[1] either "without authorization" or in a manner that "exceeds authorized access." However, Furukawa must also show that it suffered "damage"[2] or "loss" [3] as a result of Hossain's purported violation of the CFAA, and must demonstrate that the purported violation involved at least one of five

[1] A "protected computer" is defined as any computer "used in or affecting interstate or foreign commerce or communication[.]" 18 U.S.C. § 1030(e)(2)(B).

[2] The CFAA defines the term "damage" as "any impairment to the integrity or availability of data, a program, a system, or information[.]" 18 U.S.C. § 1030(e)(8).

[3] The CFAA indicates that "the term 'loss' means any reasonable cost to any victim[.]" 18 U.S.C. § 1030(11). Specifically, the CFAA explains that loss includes "the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service[.]"*Id.*

aggravating factors "set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i)." 18 U.S.C. § 1030(g). Only one factor is relevant to the present claim: 18 U.S.C. § 1030(c)(4)(A)(i)(I), which requires the showing of "loss to 1 or more persons during any 1–year period . . . aggregating at least $5,000 in value." 18 U.S.C. § 1030(c)(4)(A)(i)(I).

Thus, to set forth a proper civil claim under the CFAA based on a violation of Subsection (a)(2), Furukawa must show that Hossain: (1) intentionally accessed a computer, (2) without authorization or exceeding authorized access, and that he (3) thereby obtained information (4) from any protected computer (if the conduct involved an interstate or foreign communication), and that (5) there was loss to one or more persons during any one-year period aggregating at least $5,000 in value. *See LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1132 (9th Cir. 2009).

To successfully bring an action under the CFAA based on a violation of Subsection (a)(4), Furukawa must show that Hossain: (1) accessed a "protected computer," (2) without authorization or exceeding such authorization that was granted, (3) "knowingly" and with "intent to defraud," and thereby (4) "further[ed] the intended fraud and obtain[ed] anything of value," causing (5) a loss to one or more persons during any one-year period aggregating at least $5,000 in value. *See id.* (citing *P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC*, 428 F.3d 504, 508 (3d. Cir. 2005)).

Here, Hossain contends that he is entitled to partial judgment on the pleadings because Furukawa cannot satisfy the first and second factors of either of these inquiries. In other words, Hossain contends that Furukawa cannot show he accessed a protected computer either "without authorization" or in a manner that "exceeds authorized access." The Court disagrees.

The CFAA does not define the phrase "without authorization," however the CFAA does define "exceeds authorized access" as follows: "[T]o access a computer with authorization and to

use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). Given the similarity of the phrases, there is a deep circuit split regarding interpretations and the scope of the CFAA. The circuit split has been cast as a clash between "broad" and "narrow" interpretations of the CFAA's phrases "without authorization" and "exceeds authorized access."

The "broad" approach was first adopted by the First Circuit, which found that an employee "exceeds authorized access" by violating a confidentiality agreement. *See EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 581–84 (1st Cir. 2001). Later, the Seventh Circuit adopted a "broad" view based on principles of agency when it found that an employee acted "without authorization" as soon as the employee severed the agency relationship through disloyal activity. *See Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006).

More recently, however, courts have moved away from a "broad" view premised on theories of agency and violations of confidentiality agreements. The more recent trend for the "broad" approach finds that an employee "exceeds authorized access" by violating employer policies regarding access and use of computers. *See, e.g.*, *United States v. John*, 597 F.3d 263, 271–73 (5th Cir. 2010) ("While we do not necessarily agree that violating a confidentiality agreement . . . would give rise to criminal culpability, we do agree with the First Circuit that the concept of 'exceeds authorized access' may include exceeding the purposes for which access is 'authorized.'"); *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010); *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58, 62 (1st Cir. 2003) ("A lack of authorization could be established by an explicit statement [.]"); *see also United States v. Salum*, 257 F. App'x 225, 230 (11th Cir. 2007); *United States v. Teague*, 646 F.3d 1119, 1121–22 (8th Cir. 2011).

The Ninth Circuit was the first Circuit to adopt the "narrow" interpretation of the CFAA by narrowly interpreting the CFAA's "without authorization" language. *See LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009). In so doing, the Ninth Circuit repudiated the "broad" approach, which used principles of agency to give meaning to the CFAA's "without authorization" language. *See Brekka*, 581 F.3d at 1134. The Court in *Brekka* explicitly refused to hold an employee liable under the CFAA's "without authorization" language based on an agency theory in order to avoid interpreting the CFAA in a "surprising and novel way[] that impose[s] unexpected burdens on defendants." *Brekka*, 581 F.3d at 1134.

Instead, the Ninth Circuit in *Brekka* advanced what it deemed a "sensible" interpretation of the CFAA, giving separate meaning to the phrases "without authorization" and "exceeds authorized access" by focusing on "the employer's decision to allow or to terminate an employee's authorization to access a computer[.]" *Brekka*, 581 F.3d at 1133. In so doing, the *Brekka* decision adopted a "narrow" approach when giving meaning to the CFAA's "without authorization" language. However, to give meaning to the CFAA's "exceeds authorized access" language, the *Brekka* Court simply applied the definition provided by Congress. Under the analysis put forth by the court in *Brekka*, whether an individual "exceeds authorized access" "depends on the actions taken by the employer." *Brekka*, 581 F.3d at 1135.

In *Pulte Homes, Inc. v. Laborers' International Union of North America*, the Sixth Circuit relied heavily on the *Brekka* decision to give meaning to the CFAA's "without authorization" and "exceeds authorized access" language. 648 F.3d 295 (6th Cir. 2011). In *Pulte Homes*, the Sixth Circuit found that the phrases were separate and distinct. *See Pulte Homes*, 648 F.3d at 304 (citing *Citrin*, 440 F.3d at 420, to note "that 'the difference . . . is paper thin,'" and

citing *Daniel v. Cantrell*, 375 F.3d 377, 383 (6th Cir. 2004), to note that the Sixth Circuit can give meaning to both "without authorization" and "exceeds authorized access" under the CFAA).

The Sixth Circuit relied on the *Brekka* decision to apply a "narrow" interpretation to the CFAA's "without authorization" language. *See Pulte Homes*, 648 F.3d at 303-04. However, after recognizing a distinction between the CFAA's phrases, the Sixth Circuit did not go beyond the CFAA's provided definition to give meaning to "exceeds authorized access;" opting instead to simply apply the meaning provided by Congress, just as the Ninth Circuit did in *Brekka*. *See Pulte Homes*, 648 F.3d at 304; *cf. Brekka*, 581 F.3d at 1135. Essentially, the Sixth Circuit adopted the original "sensible" interpretation put forth by the Ninth Circuit's *Brekka* decision.

Nevertheless, the Ninth and Fourth Circuits later widened the circuit split by applying the "narrow" interpretation to give meaning to the CFAA's "exceeds authorized access" language as well. *See United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc); *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012). Under the Ninth and Fourth Circuit's new "narrow" interpretation of "exceeds authorized access," an employee given access to a computer is authorized to access the computer regardless of any policies that regulate the *use* of the computer or its information. *See Nosal*, 676 F.3d at 863-64; *WEC Carolina*, 687 F.3d at 207.

Hossain argues that the approach taken by the Ninth and Fourth Circuits is proper because they interpret both the phrases "without authorization" *and* "exceeds authorized access" narrowly. Hossain urges this Court to follow other district courts in Michigan that have followed the Ninth and Fourth Circuit's new "narrow" approach. *See, e.g., Ajuba Int'l, L.L.C. v. Saharia*, 871 F. Supp. 2d 671 (E.D. Mich. 2012); *Dana Ltd. v. Am. Axle & Mfg. Holdings, Inc.*, No. 1:10-CV-450, 2012 WL 2524008 (W.D. Mich. June 29, 2012).

However, this Court is not bound by such decisions. *See Camreta v. Greene*, 131 S. Ct. 2020, 2033 n.7, 179 L. Ed. 2d 1118 (2011)). This Court must take its guidance from the Sixth Circuit, which interpreted the CFAA's "without authorization" and "exceeds authorized access" language separately to give meaning to each phrase. *See Pulte Homes*, 648 F.3d at 303-04.

While "[d]ifferent interpretations of the same statute within the same district court are generally not preferred (except, perhaps, by courts of appeals, which were created in part to resolve such differences of opinion)[,]" *Dice Corp. v. Bold Technologies*, No. 11-13578, 2012 WL 263031, at *7 (E.D. Mich. Jan. 30, 2012), this Court will follow the guidance of the Sixth Circuit to find that a "narrow" interpretation is warranted to give meaning to the CFAA's "without authorization" language, but not "exceeds authorized access."

a. Without Authorization

The Court agrees with the other courts in this district who have adopted the "narrow" approach to give meaning to the CFAA's "without authorization" language. In light of the meaning the Sixth Circuit gave to the phrase "without authorization," this Court finds that adopting the "broad" agency approach advanced by Furukawa would be contrary to plain meaning of the CFAA. Nevertheless, even under, the "narrow" approach, the Court finds that Furukawa has properly alleged that Hossain accessed *some* files "without authorization."

i. The Sixth Circuit adopted a narrow interpretation of "without authorization," which is controlling in this Court.

Furukawa pushes the Court to adopt a "broad" agency approach to give meaning to the CFAA's "without authorization" language, arguing that "'an employee accesses a computer 'without authorization' whenever the employee, without the employer's knowledge, acquires an interest that is adverse to that of his employer or is guilty of a serious breach of loyalty." Dkt. No. 33 at 18 (quoting *GuestTek v. Interactive Entm't, Inc.*, 665 F. Supp. 2d 42, 45 (D. Mass.

2009)); *see also id.* (quoting *Citrin*, 440 F.3d at 420-21 to state: "The reasoning behind this approach is that '[v]iolating the duty of loyalty, or failing to disclose adverse interests, voids the agency relationship' and, therefore, 'terminates' the agent's 'authority.'").

This Court will not adopt a broad agency approach in light of the meaning the Sixth Circuit provided for the CFAA's "without authorization" language. Because the CFAA's "without authorization" language was not defined by Congress, the Sixth Circuit looked to term's ordinary usage. *See Pulte Homes*, 648 F.3d at 303 ("Because Congress left the interpretation of 'without authorization' to the courts, we [] start with ordinary usage.").

To define "authorization" the Sixth Circuit found that the "plain meaning of 'authorization' is '[t]he conferment of legality; . . . sanction.'" *Id.* at 303-04 (citing 1 Oxford English Dictionary 798 (2d ed. 1989)) (brackets in original). With this definition for "authorization," the Sixth Circuit definitively concluded: "Commonly understood, then, a defendant who accesses a computer 'without authorization' does so *without sanction or permission*." *Id.* (citing *Brekka*, 581 F.3d at 1132–33) (emphasis added).

The Sixth Circuit's definition of "without authorization" is in accord with other circuits that defined the term. For example, the Ninth Circuit explained that "a person who 'intentionally accesses a computer without authorization,' accesses a computer without any permission at all[.]" *Brekka*, 581 F.3d at 1133 (citing RANDOM HOUSE UNABRIDGED DICTIONARY, 139 (2001) and WEBSTER'S THIRD INTERNATIONAL DICTIONARY, 146 (2002) to define "without authorization") (internal citations omitted); *cf. WEC Carolina*, 687 F.3d 199 at 204 (citing *Oxford English Dictionary* (2d ed. 1989; online version 2012), to define "'authorization' as 'formal warrant, or sanction[,]" and citing *Brekka*, 581 F.3d at 1133, to state an employee is "'without authorization' when he gains admission to a computer without approval.").

While Furukawa argues that Hossain's authorization terminated with his alleged breach of the Secrecy Agreement, this Court disagrees. Just because an employee acquires interests adverse to their employer's, it does not inevitably follow that the employee accessed information "without authorization." Indeed, in *Brekka*—which the Sixth Circuit relies on heavily—the Ninth Circuit rejected such a "broad" agency based interpretation of the CFAA's "without authorization" language noting: "Nothing in the CFAA suggests that a defendant's liability for accessing a computer without authorization turns on whether the defendant breached a state law duty of loyalty to an employer." *Brekka*, 581 F.3d at 1135 (9th Cir. 2009). This Court agrees, and will follow the guidance of the Sixth Circuit and interpret the CFAA's "without authorization" language narrowly. *See Pulte Homes*, 648 F.3d at 304.

ii. The rule of lenity requires a "narrow" interpretation of the CFAA's "without authorization" language.

Furukawa also argues "that the 'legislative history' supports the broad view." Dkt. No. 33 (citing *Shurgard Storage Ctrs., Inc. v. Safegard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1127-29 (W.D. Wash. 2000)). The *Brekka* court rejected a "broad" agency approach to avoid interpreting the CFAA's "without authorization" language in a "surprising and novel way[] that impose[d] unexpected burdens on defendants." *Brekka*, 581 F.3d at 1134 (citing *United States v. Santos*, 553U.S. 507, 128 S.Ct. 2020, 170 L.Ed.2d 912 (2008) (J. Scalia) (plurality opinion)).

Because the CFAA is also a criminal statute, the Ninth Circuit emphasized that "[t]he rule of lenity, which is rooted in considerations of notice, requires courts to limit the reach of criminal statutes to the clear import of their text and construe any ambiguity against the government." *Id.* at 1135 (citing *United States v. Romm*, 455 F.3d 990, 1001 (9th Cir. 2006)).

The Court in *Brekka* explained that unexpected results would follow if criminal liability were to turn on principles of agency. *See id.* ("If [an] employer has not rescinded the defendant's

right to use the computer, the defendant would have no reason to know that making personal use of the company computer in breach of a state law fiduciary duty to an employer would constitute a criminal violation of the CFAA."

To avoid unexpected results with respect to interpreting "without authorization," the Ninth Circuit explicitly rejected the rational underpinning decisions finding liability under the CFAA based on an agency theory. *See Brekka*, 581 F.3d at 1135 (finding that the "interpretation [relied upon in] *Citrin* does not comport with the plain language of the CFAA, and given the care with which we must interpret criminal statutes to ensure that defendants are on notice as to which acts are criminal we decline to adopt the interpretation of 'without authorization' suggested by *Citrin.*"). Again, this Court agrees with the Ninth Circuit's opinion in *Brekka*, and finds that the rule of lenity favors a narrow construction of the CFAA's "without authorization" language.

iii. Furukawa properly alleges that Hossain took some files "without authorization"

The Sixth Circuit provided the following guidance for determining whether an individual accesses information without authorization: "We ask [] whether [the defendant] had *any* right to call [the plaintiff's] offices and email its executives." *Id.* (emphasis in original). Following the guidance of the Sixth Circuit, this Court similarly asks whether Hossain had *any* right to access the Furukawa files. This Court finds Hossain did have a right up to a certain point.

In Furukawa's Complaint, it notes that "[i]n his capacity as Production manager and Senior Production Manager, Hossain had access to Furukawa's trade secrets, know-how, intellectual property or other confidential information[.]" Dkt. No. 1 at ¶ 30. Nonetheless, Furukawa claims Hossain illegally downloaded a total of 1,785 files to his external hard drive and two-and-half years of email from Furukawa's exchange server on March 10, 2014 and March 17, 2014.

Because Hossain had access on March 10, 2014 and March 17, 2014, the Court finds that the 1,785 files and the two-and-a-half years of email Hossain downloaded from Furukawa's exchange server were not downloaded "without authorization" under the CFAA. *Cf. Pulte Homes*, 648 F.3d at 304 ("Because [the plaintiff] does not allege that [the defendant] possessed *no* right to contact [the plaintiff's] offices and its executives, it fails to satisfy one of the elements—access "without authorization"—of its claim.") (emphasis in original).

Furukawa points to its Removable Media Policy to argue Hossain illegally accessed the files on March 11, 2014 and March 17, 2014. However, the Removable Media Policy is relevant in determining whether Hossain "exceeded authorized access," on March 11, 2014 and March 17, 2014; not whether Hossain accessed the files "without authorization." Hossain's alleged disregard of the limitation put in place by the Removable Media Policy does not change the fact that Hossain was still authorized to access the files. *See Brekka*, 581 F.3d at 1133. [4]

Nevertheless, Furukawa does make a compelling point by noting that "[w]hile on leave of absence from his employment with Furukawa, [Hossain] also downloaded Furukawa's files from his company computer to an external hard drive, and copied Furukawa's files from his company email account to his personal 'gmail' account." Dkt. No. 1 at ¶ 53.

Furukawa highlights the fact that it informed Hossain he was not authorized to work during the period of March 18, 2014 to April 24, 2014. *See* Dkt. No. 33 at 21 (citing Dkt. No. 33-1 at 2-3). As a condition for granting the leave of absence, Furukawa instructed Hossain that he

[4] A helpful analogy for the application of the "narrow" interpretation of the CFAA's "without authorization" language was explained in a district court opinion out of the Eastern District of Pennsylvania:

> An analogy to burglary provides clarity . . . "If a person is invited into someone's home and steals jewelry while inside, the person has committed a crime—but not burglary—because he has not broken into the home. The fact that the person committed a crime while inside the home does not change the fact that he was given permission to enter."

Dresser-Rand Co. v. Jones, 957 F. Supp. 2d 610, 614 (E.D. Pa. 2013) (quoting Thomas E. Booms, *Hacking into Federal Court: Employee "Authorization" Under the Computer Fraud and Abuse Act*, 13 VAND. J. ENT. & TECH. L. 543, 571 (2011)).

could not do "any work" for Furukawa during his leave of absence. *See* Dkt. No. 33 at 9. An interchange during Hossain's deposition indicates that Hossain was verbally instructed he could not work for Furukawa, and that his access to his Furukawa email account and Furukawa's network was physically revoked. Dkt. No. 1-1(Deposition of Isthihar Hossain).

In light of these facts, and assuming Furukawa's allegations are true, the Court finds Hossain actually had *no* right to access files during his leave of absence. *See Pulte Homes*, 648 F.3d at 305; *see also Brekka*, 581 F.3d at 1136 (9th Cir. 2009) ("There is no dispute that if [the defendant] accessed [the company's] information . . . after he left the company . . ., [the defendant] would have accessed a protected computer 'without authorization' for purposes of the CFAA."); *United States v. Steele*, 595 F. App'x 208, 211 (4th Cir. 2014) ("[T]he fact that [the defendant] no longer worked for [the company] when he accessed its server logically suggests that the authorization he enjoyed during his employment no longer existed.").[5]

Accordingly, the Court finds that the 1,785 files and the two-and-a-half years of email Hossain downloaded to his external hard drive from Furukawa's exchange server on March 10, 2014 and March 17, 2014 were *not* downloaded "without authorization" under the CFAA. However, because there were files allegedly downloaded without *any* permission during Hossain's leave of absence, the Court finds that Hossain is not entitled to judgment on the pleadings for the CFAA claim as it pertains to accessing some files "without authorization."

[5] The Court is aware that Hossain was still employed by Furukawa while on his leave of absence, this does not overshadow the fact that Furukawa took overt steps to revoke Hossain's access such that he would recognize he was "without authorization." *See, e.g.*, *Steele*, 595 F. App'x at 211 (noting the defendant in that case "clearly acted 'without authorization' under the plain meaning of the CFAA" because: "Common sense aside, the evidence provides ample support for the jury's verdict. [The company] took steps to revoke [the defendant's] access to company information, including collecting [the defendant's] company-issued laptop, denying him physical access to the company's offices, and generally terminating his main system access. And [the defendant] himself recognized that his resignation effectively terminated any authority he had to access [the company's] server, promising in his resignation letter that he would not attempt to access the system thereafter. Just because [the company] neglected to change a password on [the defendant's] backdoor account does not mean [the company] intended for [the defendant] to have continued access to its information.").

a. Exceeds Authorized Access

This Court will depart from the other district courts in Michigan that have found the Sixth Circuit favors a narrow approach to both the phrases "without authorization" *and* "exceeds authorized access." This Court finds that the Sixth Circuit's narrow approach does not extend to the CFAA's "exceeds authorized access" language, because the Sixth Circuit relied on the unambiguous definition provided for the phrase. Accordingly, this Court finds that Furukawa properly alleged that Hossain "exceeded authorized access" by downloading Furukawa files in contravention of the Removable Media Policy.

i. The Sixth Circuit adopted the unambiguous definition of "exceeds authorized access" provided by Congress in the CFAA. Nothing in the definition provided by Congress forecloses employers from implementing computer polices that restrict both access and use.

As discussed, the Sixth Circuit recognized the distinction between the CFAA's phrases "without authorization" and "exceeds authorized access." *Pulte Homes*, 648 F.3d at 304 (citing *Citrin,* 440 F.3d at 420and citing *Cantrell*, 375 F.3d at 383). This distinction is important because the Sixth Circuit's opinion in *Pulte Homes* only adopted the "narrow" approach as it pertained to interpreting the phrase "without authorization;" not "exceeds authorized access." *See Pulte Homes*, 648 F.3d at 304; *see also Dana Ltd.*, 2012 WL 2524008, at *3 ("[T]he Sixth Circuit's opinion in *Pulte Homes*, suggests that the Sixth Circuit would adopt the narrow view insofar as it relied heavily on the ninth Circuit's opinion in LVRC Holdings *for a definition of 'without authorization*.'") (emphasis added) (internal citation committed).

With respect to the phrase "exceeds authorized access," the Sixth Circuit did not go beyond the plain language of the CFAA's provided language. *See Pulte Homes*, 648 F.3d at 304 (citing 18 U.S.C. § 1030(e)(6) to note: "Unlike the phrase 'without authorization,' the CFAA helpfully defines 'exceeds authorized access'"). The Sixth Circuit cited the Ninth Circuit's

opinion in *Brekka* to analyze the CFAA's definition of "exceeds authorized access" and note: "Under this definition, 'an individual who is authorized to use a computer for certain purposes *but goes beyond those limitations* . . . has 'exceed[ed] authorized access.'" *Pulte Homes*, 648 F.3d at 304 (quoting *Brekka*, 581 F.3d at 1133); *cf. Brekka*, 581 F.3d at 1133 (interpreting only the phrase "without authorization," yet looking to the plain language of the phrase "exceeded authorized access" to reach "a sensible interpretation of §§ 1030(a)(2) and (4)[.]").

The Sixth Circuit never indicated that limitations on employee access and use of employer computers were foreclosed by the CFAA. Thus, this Court disagrees with the court decisions cited by Hossain that take a "narrow" approach to the CFAA's "exceeds authorized access" language in order to find that there can be no liability for an individual who violates a computer use policy. *See*, *e.g.*, *Dana*, WL 2524008, at *4 (citing *Nosal*, 676 F.3d at 859, for the proposition that "[f]ederal criminal liability should not be based on every violation of a private computer use policy."); *Ajuba*, 871 F. Supp. 2d at 685-88 (narrowly interpreting "exceeds authorized access" to dismiss a CFAA claim where the employer alleged an employee exceeded his authorization by accessing computers in violation of use limitations).

The Ninth Circuit opinion from which the courts taking a narrow approach base their reasoning is out of step with the findings of the Sixth Circuit. While the Sixth Circuit simply looked to definition provided by Congress to interpret the CFAA's "exceeds authorized access" language, the Ninth Circuit panel in *Nosal* looked beyond the definition provided by Congress to the legislative history of the CFAA to interpret the phrase. *See Nosal*, 676 F.3d at 860.

In *Nosal*, the United States ("the government") sought to enforce a computer policy focused on access, purpose, and use. *See* Reply Brief for Petitioner Appellant, *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc) (No. 10-10038), 2010 WL 6191782, at *3. The

government argued that the employees in *Nosal* were liable under the CFAA because the company "granted [the employees] a restricted right to access [the company] computers by explicitly instructing [the employees] to access information in the Searcher database only for legitimate [company] business purposes." *Id.* at *3. According to the government, "[w]hen [the employees] accessed the Searcher database for other purposes, they violated this express access restriction and thereby obtained proprietary [company] information that they were 'not entitled so to obtain.'" *Id.* (citing 18 U.S.C. § 1030(e)(6)).

The *Nosal* panel disagreed and found that "'exceeds authorized access' in the CFAA is limited to violations of restrictions on *access* to information, and not restrictions on its *use*." *Nosal*, 676 F.3d at 864. To reach its decision, the *Nosal* panel claimed "to follow in the path blazed by *Brekka*[.]" *Id.* at 863. To the contrary, however, the *Nosal* panel parted from the path blazed by *Brekka* by refusing to emphasize the plain language of the CFAA and resorting to an unnecessary analysis of the CFAA's legislative history. In so doing, the panel took "a plainly written statute and pars[ed] it in a hyper-complicated way that distort[ed] the obvious intent of Congress." *United States v. Nosal*, 676 F.3d 854, 864 (9th Cir. 2012) (Silverman, J., dissenting).

The *Nosal* panel ignored the "sensible interpretation of [the CFAA]" put forth in *Brekka* that relied on the plain language of the CFAA. *See Brekka*, 581 F.3d at 1133. In *Brekka*, the Ninth Circuit used the CFAA's plain language to describe "a person who 'exceeds authorized access'" as a person who "has permission to access the computer, but accesses information on the computer that *the person is not entitled to access*." *Id.* (emphasis added).

As the government argued in *Nosal*, the operative term in the CFAA's definition of "exceeds authorized access" is "entitled," which is defined by *Webster's New Riverside University Dictionary* as "to furnish with a right." Brief for Petitioner Appellant, *United States v.*

Nosal, 676 F.3d 854 (9th Cir. 2012) (en banc) (No. 10-10038), 2010 WL 6191778, at *15 (citing *Webster's New Riverside University Dictionary* 435). As the government explained, "[s]ince the employer furnishes the right to access its computer systems and obtain information from it, explicit policies restricting the right to obtain information from workplace computers determines when an individual 'exceeds authorized access.'" *Id.*

The government further highlighted that the term "so" in definition provided for "exceeds authorized access" was defined as "[i]n the state or manner indicated or expressed." Reply Brief for Petitioner Appellant, *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc) (No. 10-10038), 2010 WL 6191782, at *8 (quoting *Webster's II New Riverside University Dictionary* 1102 (1988)). By noting that the provided definition of "exceeds authorized access" focused on *the manner* of access, the government explained that the provided definition means "someone exceeds authorized access when he obtains or alters information that he is not entitled to obtain or alter *in those circumstances*." *Id.* (citing 18 U.S.C. § 1030(e)(6)) (emphasis in original).

Essentially, the government argued that the provided definition comports with the Sixth Circuit's finding that "'an individual who is authorized to use a computer for certain purposes *but goes beyond those limitations* . . . has 'exceed[ed] authorized access.'" *Pulte Homes*, 648 F.3d at 304 (quoting *Brekka*, 581 F.3d at 1133); *cf.* Reply Brief for Petitioner Appellant, 2010 WL 6191782, at *9 ("[T]he definition of 'exceeds authorized access' shows that someone exceeds authorized access by obtaining information *in a prohibited manner*, even if the accesser might be entitled to obtain the same information under other circumstances.") (emphasis added).

Nevertheless, the *Nosal* panel disagreed, finding that computer policies focused on use were "a poor fit with the statutory language [of the CFAA]." *Nosal*, 676 F.3d at 857. Instead, the *Nosal* panel found that in the provided definition of "exceeds authorized access," "[a]n equally

or more sensible reading of 'entitled' is as a synonym for 'authorized.'" *Id.* The *Nosal* panel then found that the government placed "a great deal of weight on a two-letter word that is essentially a conjunction," before finding that "the government's 'so' argument [didn't] work because the word has meaning even if it doesn't refer to use restrictions." *Nosal*, 767 F.3d at 857-58.

Thus, rather than address the government's argument, which focused on the manner of access, the *Nosal* panel discounted the argument because it found "Congress could . . . have included 'so' as a connector or for emphasis." *Id.* at 858. This Court does not believe the Sixth Circuit would take the *Nosal* panel's approach. By inflexibly focusing only on the government's defining of the word "so," the *Nosal* panel missed the overarching point that the government was attempting to make: that someone exceeds authorized access by obtaining information in a prohibited manner, even if the accesser might be entitled to obtain the same information under other circumstances. *See* Reply Brief for Petitioner Appellant, 2010 WL 6191782, at *9.

The *Nosal* panel seemed to imply that the manner in which an individual accesses information is inconsequential after providing the following hypothetical to explain why the government's "so" argument purportedly didn't work:

> Suppose an employer keeps certain information in a separate database that can be viewed on a computer screen, but not copied or downloaded. If an employee circumvents the security measures, copies the information to a thumb drive and walks out of the building with it in his pocket, he would then have obtained access to information in the computer that he is not "entitled *so* to obtain."

Nosal, 676 F.3d at 858. However, in its hypothetical, the *Nosal* panel suggests that an employer is certainly able to bring an action against an individual under the CFAA if the individual accesses the employer's computers in a manner that exceeds "security measures."

This Court fails to see a difference between an employee who circumvents "security measures," and an employee who circumvents explicit computer limitations provided by an

employer for employees regarding the employee's access, use, or purpose when accessing the employer's systems. To this Court, such explicit policies are nothing but "security measures" employers may implement to prevent individuals from doing things in an improper manner on the employer's computer systems.

Such a view is in accord with the plain language of the statute. Indeed, the *Nosal* panel acknowledged that employer policies restricting the manner of use and access fit the plain language of the CFAA. *See Nosal*, 767 F.3d at 858 ("[T]he CFAA is susceptible to the government's broad interpretation[.]"). Nevertheless, the *Nosal* panel explicitly rejected this idea, finding that "it is possible to read both prohibitions as applying to hackers." *Id.*

According to the *Nosal* panel: "'[W]ithout authorization' would apply to *outside* hackers (individuals who have no authorized access to the computer at all) and 'exceeds authorized access' would apply to *inside* hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files)." *Id.* But this "outside hacker" and "inside hacker" distinction fails to account for the employer's ability to dictate the manner in which "inside hackers" access unauthorized information or files.

As discussed, the Sixth Circuit in *Pulte Homes* adopted the *Brekka* approach to make clear that an individual only acts "without authorization" when they are *completely* prohibited from accessing, obtaining, or altering anything on a protected computer, *in any manner*. Thus, an employee's "authorized access" is completely dependent on the scope of the authorization provided by employers, who dictate at a threshold level how and what an employee may properly access, obtain, or alter on the employer's computer. As the dissent in *Nosal* explained, "[t]his is not an esoteric concept." *Nosal*, 676 F.3d at 865 (Silverman, J., dissenting). Indeed, the concept was originally advanced by the Ninth Circuit in *Brekka* when they acknowledged that "[t]he

plain language of the statute [] dictates that 'authorization' depends on the *actions taken by the employer*." *Brekka*, 581 F.3d at 1135 (emphasis added).

The Court in *Brekka* explained that, "for purposes of the CFAA, when an employer authorizes an employee to use a company computer subject to certain limitations, the employee *remains authorized to use the computer* even if the employee violates those limitations." *Brekka* 581 F.3d at 1133 (emphasis added). Because an individual can violate employer-placed limits, yet still have authorization to access an employer's computer; limitations dictating the manner in which the employee may properly access, obtain or alter information on the computer, give full effect to the CFAA's "exceeds authorized access" language.[6]

Foreclosing purpose and use restrictions by employers, simply conflicts with the plain language of the statute. *See Nosal*, 676 F.3d at 864 (Silverman, J., dissenting). If an employee were to take customer information in violation of a use policy to commit widespread identity theft, it would still be the work of an "inside hacker." *Cf. United States v. John*, 597 F.3d 263, 271-73 (5th Cir. 2010) (finding an employee of Citigroup exceeded her authorized access in violation of the CFAA when she accessed confidential customer information in violation of her employer's computer use restrictions and used that information to commit fraud).

Moreover, the CFAA provides an avenue to obtain civil relief against this "inside hacker," regardless of whether the employee's actions were part of a criminal scheme. *Cf. United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010) (rejecting the argument that the Defendant should not be liable under the CFAA because his conduct was "not criminal," and

[6] For example, a company may explicitly instruct a driver that he/she can only access the company's car to deliver the company's pizzas; provided the driver delivers the pizzas *in the manner* the company dictates he/she can use the company's car. The driver's access to the car—the driver's entitlement/authorization—will remain so long as the driver does not go beyond the instructions provided by the company regarding the use of the car. However, the driver would not be entitled/authorized—the driver would "exceed authorized access"—to use the company's car to deliver a competing company's pizza; sell drugs out of the company's car; or do anything else beyond of the scope of *how* the driver was instructed to use the company's car.

noting: "The problem with [the defendant's] argument is that his *use of information is irrelevant if he obtained the information without authorization or as a result of exceeding authorized access*.") (emphasis added).

The *Nosal* panel never clearly explains why the CFAA's plain language does not permit computer owners to "spell out explicitly what is forbidden" on its computers. *See EF Cultural Travel B.V. v. Zefer Corp.*, 318 F.3d 58, 63 (1st Cir. 2003); *see also United States v. John*, 597 F.3d at 271–73; *United States v. Rodriguez*, 628 F.3d at 1263; *United States v. Salum*, 257 F. App'x at 230; *United States v. Teague*, 646 F.3d at 1121–22. Indeed, that was the interpretation *originally* adopted by the Ninth Circuit. *See Brekka*, 581 F.3d at 1135. Accordingly, this Court finds that the Sixth Circuit would look to the provided definition under the CFAA to find that whether an employee "exceeds authorized access," depends on actions taken by the employer.

ii. There is no need to apply the rule of lenity to interpret the CFAA's "exceeds authorized access" language because Congress provided a clear and unambiguous definition for the phrase.

The Court's inquiry should end with the unambiguous definition provided by Congress for "exceeds authorized access" because "[i]f the statute is not ambiguous, the use of canons of construction, reference to legislative history, and application of the rule of lenity is not appropriate." *United States v. Lumbard*, No. 1:10-CR-388, 2011 WL 4704890, at *1 (W.D. Mich. Oct. 6, 2011) *aff'd*, 706 F.3d 716 (6th Cir. 2013); *see also Dep't of Housing and Urban Dev. v. Rucker*, 535 U.S. 125, 132, 122 S.Ct. 1230, 152 L.Ed.2d 258 (2002); *United States v. Johnson*, 529 U.S. 53, 59, 120 S.Ct. 1114, 146 L.Ed.2d 39 (2000).

Both the Supreme Court of the United States and Sixth Circuit have noted that the rule of lenity only "comes into operation *at the end* of the process of construing what Congress has expressed, not at the beginning as an overriding consideration of being lenient to wrongdoers."

United States v. Adams, 722 F.3d 788, 804 n.8 (6th Cir. 2013) (quoting *Callanan v. United States*, 364 U.S. 587, 596, 81 S.Ct. 321, 5 L.Ed.2d 312 (1961)) (emphasis added).

The *Nosal* panel never explained how the CFAA's definition for "exceeds authorized access" was ambiguous, yet the panel examined the legislative history of the CFAA to conclude: "If Congress meant to expand the scope of criminal liability to everyone who uses a computer in violation of computer use restrictions . . . *we would expect it to use language better suited to that purpose*." *Nosal*, 676 F.3d at 857 (emphasis added); *see also id.* at 857 n.3 (citing 18 U.S.C. § 1832(a) to note Congress did, in fact, use specific language "in the federal trade secrets statute [] where it used the common law terms for misappropriation[.]); *id.* at 858 (stating that the "narrow" construction of "exceeds authorized access is a "perfectly plausible construction of the statutory language" that does not turn the CFAA "into a sweeping Internet-policing mandate."); *id.* at 858 n.5 (outlining the legislative history to support the "narrow" construction).

However, the judiciary's "expectation" that Congress would use "better suited" language is not an excuse to encroach upon powers explicitly reserved to the legislative branch. *See Violette v. P.A. Days, Inc.*, 427 F.3d 1015, 1017 (6th Cir. 2005) (quoting *Rucker*, 535 U.S. at 134-35, to note: "To avoid a law's plain meaning in the absence of ambiguity 'would trench upon the legislative powers vested in Congress by Art. I, § 1, of the Constitution.'"). Unlike the *Nosal* panel, this Court will not read ambiguity into the definition of "exceeds authorized access" at the beginning of its analysis "as an overriding consideration of being lenient to wrongdoers." *Adams*, 722 F.3d at 804 n.8 (quoting *Callanan v. United States*, 364 U.S. at 596).

The *Nosal* panel resorted to the CFAA's legislative history to apply the rule of lenity due to concerns that "millions of unsuspecting individuals would find that they are engaging in criminal conduct." *Nosal*, 676 F.3d at 859; *see also id.* at 860 (worrying that "[b]asing criminal

liability on violations of private computer use polices can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved[,]" and worrying that a broad reading of the CFAA could turn "minor dalliances" into "federal crimes").

The *Nosal* panel's concern was rooted in the fact that "[w]hile it's unlikely that you'll be prosecuted for [innocuous conduct] on your work computer, you *could* be." *Nosal*, 676 F.3d at 860 (emphasis in original); *see id.* at 860 n.7 (providing a hypothetical of an aggressive prosecutor who might attempt to prosecute an employee who spends six hours a day tending to his FarmVille stable on his work computer in violation of the company's use policy).[7]

The *Nosal* panel sought to narrow the definition of "exceeds authorized access" in order to "consider how the interpretation [] will operate wherever in [the CFAA] the phrase appears." *Nosal*, 676 F.3d at 859; *see also id.* (noting that the "phrase appears five times in the first seven subsections of the statute, including subsection 1030(a)(2)(C)"). The panel paid specific attention to Subsection (a)(2)(c), which it labeled as "the broadest" provision because Subsection (a)(2)(c) makes it a crime to access a computer "*without* any culpable intent." *Nosal*, 676 F.3d 859.[8]

Under Subsection (a)(2)(c), the *Nosal* panel found that "the broad interpretation of the CFAA" would allow "private parties to manipulate their computer-use and personal policies so as to turn these relationships into ones policed by the criminal law." *Nosal*, 676 F.3d at 860; *see*

[7] However, this concern does not warrant avoiding a definition provided by Congress. The Court agrees prosecuting an individual for using his FarmVille account at his job "does not appear to be a worthy way to expend valuable law enforcement resources." *Lawrence v. Texas*, 539 U.S. 558, 605, 123 S. Ct. 2472, 156 L. Ed. 2d 508 (2003) (Thomas, J., dissenting). Nevertheless, just because inane prosecutions are possible, it does not mean that the statutes underlying the prosecutions are flawed.

[8] However, this concern is overstated because liability under the CFAA will not attach unless an individual accesses a computer *and* obtains something to which they are not entitled. So even if an individual exceeds authorized access by accessing Facebook in a wrongful manner, in order for liability to attach the individual would *still* have to obtain something to which they were not entitled so to obtain or alter. *See, e.g., Lee v. PMSI, Inc.*, No. 8:10-CV-2904-T-23TBM, 2011 WL 1742028, at *2 (M.D. Fla. May 6, 2011) ("Because the only information [the employee] allegedly accessed was on [] personal websites, not [the employer's]computer system, [the employee] never 'obtained or alter[ed] information in the computer.' [The employee] accessed her facebook, personal email, and news websites but did not access any information that she was 'not entitled so to obtain or alter.').

also id. at 860 n.6 (noting that "[e]nforcement of the CFAA against minor workplace dalliances is not chimerical," and stating that a district court case from Florida—where an employer brought claims against an employee under the CFAA—could not have been dismissed if "exceeds authorized access included violations of private computer use policies.").[9]

Thus, to quell its concerns, the *Nosal* panel rejected the Government's position that the CFAA's definition of the phrase "exceeds authorized access" includes use restrictions. *Nosal*, 676 F.3d at 875-58. Instead, to avoid a harsh construction, the *Nosal* panel found that the phrase "exceeds authorized access" only applies to someone who accesses data that the accesser is completely prohibited from obtaining at all, in any manner. *See Nosal*, 676 F.3d at 864.

The Fourth Circuit agreed with the *Nosal* panel, but labeled the Ninth Circuit's approach the "harsher approach." *WEC Carolina*, 687 F.3d at 206. The Fourth Circuit found that Congress did not "clearly intend to criminalize" behavior such as "an employee who with commendable intentions disregards his employer's policy against downloading information to a personal computer so that he can work at home and make headway in meeting his employer's goal." *Id.*[10]

Despite the unambiguous definition provided by Congress, the *Nosal* panel and the Fourth Circuit resorted to the rule of lenity because they felt Congress *clearly* meant for the CFAA's "exceeds authorized access" language to be limited to violations of restrictions on

[9] However, the Florida case *could* have been dismissed if "exceeds authorized access included violations of private computer use policies." It is important to note that *Lee v. PMSI, Inc.* was a civil action. No. 8:10-CV-2904-T-23TBM, 2011 WL 1742028 (M.D. Fla. May 6, 2011). The *Nosal* panel does not account for the fact that, in order to be civilly liable that under CFAA, there must be damage or loss to one or more persons during any one-year period aggregating to at least $5,000 in value. *See* 18 U.S.C. § 1030(c)(4)(A)(i)(I). Indeed, the counterclaim by the employer in *PMSI, Inc.* was dismissed, in part, because the employer could not show there was sufficient damage or loss caused by the employee simply accessing Facebook at work. *See PMSI, Inc.*, 2011 WL 1742028, at *1 ("The [CFAA] does not contemplate 'lost productivity' of an employee, and with the exception of the loss of productivity, the defendant fails to allege 'damage' caused by the plaintiff's internet usage.").

[10] Again, however, this concern does not warrant avoiding a definition provided by Congress. The Court agrees that such a prosecution by a federal prosecutor would be silly. Nevertheless, this Court must decide this case based on CFAA as Congress unambiguously wrote it; "[i]t is the essence of judicial duty to subordinate [this Court's] own personal views, [and] ideas of what legislation is wise and what is not." *Griswold v. Connecticut*, 381 U.S. 479, 530-31, 85 S. Ct. 1678, 14 L. Ed. 2d 510 (1965) (Stewart, J. dissenting).

access to information. *See Nosal*, 676 F.3d at 863; *WEC Carolina*, 687 F.3d at 206. However, the *Nosal* panel and Fourth Circuit only point out that ridiculous prosecution may occur by including use restrictions; they do not point to any ambiguity in the definition of "exceeds authorized access" provided by Congress.

Given the circumstances, the *Nosal* panel and Fourth Circuit were well-intentioned by seeking to prevent harsh results. However, both the Supreme Court and the Sixth Circuit have cautioned that "[t]he judiciary is not 'licensed to attempt to soften the clear import of Congress' chosen words whenever a court believes those words lead to a harsh result.'" *Id.* (quoting *United States v. Locke*, 471 U.S. 84, 95, 105 S.Ct. 1785, 85 L.Ed.2d 64 (1985). All told, "[w]here there is no ambiguity, as is the case here, 'the rule of lenity does not come into play.'" *United States v. Adams*, 722 F.3d at 804 n.8 (quoting *United States v. Turkette*, 452 U.S. 576, 587 n.10, 101 S. Ct. 2524, 69 L. Ed. 2d 246 (1981)).

The rule of lenity does not apply here, as both the Supreme Court and Sixth Circuit have cautioned that the rule of lenity "only serves as an aid for resolving an ambiguity; *it is not to be used to beget one*." *Adams*, 722 F.3d at 804 n.8 (6th Cir. 2013) (quoting *Callanan v. United States*, 364 U.S. at 596) (emphasis added). The Sixth Circuit found no ambiguity in the CFAA's definition for "exceeds authorized access," and searching for or creating possible contrary intent is unwarranted. *P.A. Days, Inc.*, 427 F.3d at 1017 (quoting *Am. Tobacco Co. v. Patterson*, 456 U.S. 63, 75, 102 S.Ct. 1534, 71 L.Ed.2d 748 (1982), to caution that "[g]oing behind the plain language of a statute in search of a possibly contrary congressional intent is a step to be taken cautiously *even under the best of circumstances*."). The intent of Congress is clear given the plain language of CFAA's definition of "exceeds authorized access," and the Court need not look beyond the definition provided by Congress to determine its intent.

iii. Furukawa properly alleges that Hossain "exceeded authorized access" in order to take files.

Here, Furukawa has a Removable Media Policy that explicitly requires permission from a manager before accessing files with removable media. *See* Dkt. No. 1-4. Even under the "narrow" approach advanced by the *Nosal* panel and Fourth Circuit, Hossain would have exceeded authorized access because he removed files in violation of a policy that was focused on how Hossain accessed Furukawa files. This being the case, the Court finds that Furukawa has properly stated a claim under the CFAA that Hossain "exceeded authorized access" by downloading a total of 1,785 files to his external hard drive and two-and-half-years of email from Furukawa's exchange server files on March 11, 2014 and March 17, 2014.

2. The Michigan Uniform Trade Secrets Act ("MUTSA") Does Not Preempt Furukawa's Claims Pursuant To Michigan Law.

Section 8 of the Michigan Uniform Trade Secrets Act ("MUTSA") preempts claims based on conflicting state tort law and provides civil remedies for misappropriation of trade secrets. *See* Mich. Comp. Laws § 445.1908(1); *Wysong Corp. v. M.I. Industries*, 412 F.Supp.2d 612, 622–23 (E.D. Mich. 2005). However, the MUTSA does not preempt "[o]ther civil remedies that are not based upon misappropriation of a trade secret." Mich. Comp. Laws. § 445.1908(2).

The critical inquiry for courts in determining whether a claim is displaced by the MUTSA is whether the claim in question is based *solely* on the misappropriation of a trade secret. *See Dura Global Technologies, Inc. v. Magna Donnelly Corp.*, No. 07-10945, 2009 WL 3032594, at *3 (E.D. Mich. Sept. 18, 2009) (quoting *Bliss Clearing Niagara, Inc. v. Midwest Brake Bond Co.*, 270 F .Supp.2d 943 (W.D. Mich. 2003)).

If a claim is based solely upon the misappropriation of a trade secret, "the claim must be dismissed." *Bliss Clearing Niagara, Inc.*, 270 F .Supp.2d at 947; *see also Dura Global*

Technologies, Inc., WL 3032594, at *3. Conversely, where "a cause of action exists in the commercial area *not* dependent on trade secrets, that cause continues to exist." *Id.*; *see also Dura Global Technologies, Inc.*, WL 3032594, at *3.

Here, Hossain argues that Furukawa's "Fraud, Breach of Fiduciary Duty, and Conversion claims [] are based on alleged trade secret misappropriation and are preempted [by] Michigan's Trade Secret Act[.]" Dkt. No. 30 at 14 (citing Mich. Comp. Laws § 445.1908(a)). However, Hossain's argument fails because Furukawa's Breach of Fiduciary Duty and Conversion Claims are not "solely based on misappropriation of a trade secret." *Wysong*, 412 F.Supp.2d at 623.

Furukawa argues it is "also suing for tortious conduct that does not involve misappropriation of information[.]" Dkt. No. 33 at 25. Notably, Hossain actually supports Furukawa's assertion by acknowledging Furukawa's claims support causes of action beyond just the misappropriation of trade secrets.[11]

This being the case, this Court finds that the Complaint alleges facts, independent of the MUTSA claim, supporting causes of action for Fraud, Breach of Fiduciary Duty, and Conversion. *See McKesson Med.-Surgical, Inc. v. Micro Bio-Medics, Inc.*, 266 F.Supp.2d 590, 600 (E.D. Mich. 2003) (finding MUTSA did not preempt a claim because the plaintiff's claim "both according to its Complaint and its Response to Defendants' Motion, [is] based not only on [the plaintiff's] trade secrets, but also other confidential information."); *see also Lube USA Inc.*, 2009 WL 2777332, at *8; *Dura Global Technologies, Inc.*, 2009 WL 3032594, at *5.

[11] *See, e.g.*, Dkt. No. 30 at 15 (Hossain citing Dkt. No. 1 at ¶ 115 to note: "Plaintiff's fraud claim alleges that Plaintiff relied on Mr. Hossain's representations by allowing him to have access to trade secret and confidential and proprietary information *which led to unfair competition* . . . .") (emphasis added); *id.* (Hossain citing Dkt. No. 1 at ¶ 128 to note: "Plaintiff's breach of fiduciary duty claim, alleges that Mr. Hossain violated a purported duty of good faith and loyalty by using Plaintiff's trade secrets *and other information to divert business away from Plaintiff and assist[] Huatong to compete against Plaintiff.*") (emphasis added); *id.* at 16 (Hossain citing Dkt. No. 1 at ¶¶ 144-45 to note: "Plaintiff's conversion claim alleges Mr. Hossain had access to Plaintiff's trade secret *and other confidential information* . . . ."). (emphasis added).

3. Furukawa's Employment Handbook Does Not Affect Furukawa's Breach Of Contract Claim.

In Michigan, if "contract language is clear and unambiguous, its meaning is a question of law." *Gerken Paving Inc. v. LaSalle Grp. Inc.*, No. 10-CV-14905, 2012 WL 3079249, at *4 (E.D. Mich. July 30, 2012) *aff'd*, 558 F. App'x 510 (6th Cir. 2014) (quoting *Port Huron Educ. Ass'n v. Port Huron Area Sch. Dist.*, 452 Mich. 309, 550 N.W.2d 228, 237 (1996)).

Hossain argues that Furukawa bases its Breach of Contract claim on documents that are not enforceable contracts by their express terms, because Furukawa's "Policies and Practices Handbook" explicitly notes that "the adoption of this employee handbook is entirely voluntary on the part of the company and shall not be construed as creating a contractual relationship between the company and any employee. It is neither a contract nor an agreement of employment for a definite period of time[.]" Dkt. No. 30 at 17 n.3 (quoting Dkt. No. 1-3 at 26).

However, the Court need not address the Polices and Practice Handbook with respect to the Breach of Contract claim because Furukawa's Breach of Contract Claim is only premised on the "Invention Assignment & Secrecy Agreement," *see* Dkt. No. 1 at ¶ 120, and, impliedly, Furukawa's Removable Media Policy. *See id.* at ¶122. Hossain argues that Furukawa's Removable Use Policy is only a "guide," but the Court sees nothing in the Removable Media Use Policy indicating it is meant to be a guide by its express terms. *See* Dkt. No. 1-4 at 2. Moreover, Hossain does not even address the Invention Assignment & Secrecy Agreement as it pertains to the Breach of Contract claim. *See* Dkt. No. 40 at 18 (arguing that the Breach of Contract claim should be dismissed "to the extent it relies upon exhibits 1, 2, and 3[.]"). Thus, the Court finds nothing in the Removable Media Policy nor the Invention Assignment & Secrecy Agreement that warrants the dismissal of Furukawa's Breach of Contract claim.

4. Furukawa's Conversion Claim Is Properly Alleged Where Hossain Allegedly Took Emails From Furukawa's Servers.

In Michigan, conversion arises from "any distinct act of domain wrongfully exerted over another's personal property in denial of or inconsistent with the rights therein." *Llewellyn-Jones v. Metro Prop. Grp., LLC*, No. 13-11977, 2014 WL 2214209 (E.D. Mich. May 27, 2014) (citing *Foremost Ins. Co. v. Allstate Ins. Co.*, 439 Mich. 378, 391, 486 N.W.2d 600 (1992)); *see also Murray Hill Publ'ns, Inc. v. ABC Commc'ns, Inc.*, 264 F.3d 622, 636–37 (6th Cir. 2001).

Hossain argues that Furukawa's conversion claim should be dismissed because Furukawa "attached various email communications from companies and individuals who are distinct and unrelated" to Furukawa to support the claim for Conversion. *See* Dkt. No. 30 at 18. The Court disagrees. The Court points out that *all* of the documents and information allegedly removed were removed from Furukawa's servers. As Furukawa points out, "[t]he fact that some of the information 'pertains to third parties unrelated to Plaintiff,' does not negate the information as being personal property belonging to [Furukawa]; nor has [Hossain] cited any authority for that proposition." Dkt. No. 33 at 28.

Indeed, "Michigan appellate courts have held that certain intangible property can be the subject of a conversion action." *Sarver v. Detroit Edison Co.*, 225 Mich. App. 580, 586, 571 N.W.2d 759, 762 (1997) (citations omitted). In each case where the Michigan courts have found that the intangible property can be the subject of a conversion action, "the plaintiff's ownership interest in intangible property was represented by or connected with something tangible." *Id.*

Here, even though *some* emails on the server contain information pertaining to third parties, the emails were still sent to Furukawa, stored inside Furukawa's tangible property, and constituted trade secrets. *See Wysong*, 412 F. Supp. 2d at 630 ("the plaintiff's supplier contact data meets the definition of a protectable trade secret); *id.* at 629 ("customer lists developed by a

former employee and information relating to a customer's needs are not "trade secrets" under the MUTSA, *unless the employee is bound by a confidentiality agreement*.") (emphasis added). Accordingly, looking at the Complaint in a light most favorable to Furukawa, Furukawa has set forth a proper claim for conversion since Hossain took 1,785 files and two-and-half-years of email from Furukawa's exchange server and placed the information on his external hard drive.

VI. CONCLUSION

For the reasons discussed, the Court **DENIES** Defendant Hossain's Motion for Partial Judgment on the Pleadings [30].

SO ORDERED.

Dated: May 6, 2015

/s/Gershwin A Drain
HON. GERSHWIN A. DRAIN
United States District Court Judge